Disaster Management System as an Element of Risk Management for Natural Disaster Systems Using the PESTLE Framework

Abstract. Recently, we have witnessed son many natural catastrophies such as earthquakes in Japan, severe floods in the UK, US and many other parts of the world. In addition businesses have been losing tens of billions of dollars because there have been various natural and man-made disasters. However, the Disaster Management System (DMS) and system that have been put in place have proven important means of reducing the risk of damages to businesses, in particular. The DMS can minimize and in some cases, eliminates the risks through technical, management or operational solutions (risk management effort). However, it is virtually impossible to eliminate all risks. Information technology systems, for example, are vulnerable to a variety of disruptions (e.g. short-term power outage, disk drive failure) from a variety of sources such as natural disasters to terrorist actions. In many cases, critical resources may reside outside the organizations control (such as telecommunications or electric power), and the organization may be unable to ensure their availability. This study proposes a model for Disaster Management System as an Element of Risk Management using the PESTLE framework. Thus, an effective Disaster Management System in the form of contingency planning, execution and testing are essential to mitigate the risk of system and service availability. We have developed a global model for Disaster recover planning and management based on the PESTLE framework which can be customized and applied to a variety of disasters prone systems such natural, emergency, IT/Network/Security, Data recovery, and incident-response systems. The main aspect of this model has been currently used and evaluated.

Keywords: *Disaster preparedness; Disaster Management System; Recovery/Reconstruction; Risk identification; Emergency management and early warning; PESTLE*

I. INTRODUCTION

Threats and risks are increasing and becoming more difficult complex situations and these threats are becoming multifaceted and over the years have exacerbated and become difficult and dangerous situations. These threats faced today are not only transnational threats due to terrorism, globalised diseased outbreaks, critical infrastructure, eliminate changes, interdependencies and further more with the increased level of cyber-attacks. The issues that are raised through this analysis will significantly highlight the scope and severity regarding cross jurisdictional lines, which are in-line with addressing the increasing base which looks at focusing on the significant human and economic losses. This paper aims to take a very different approach to Disaster Management System as it is uses the basic principles of PESTLE and applies those to a DMS in order to improve the overall DMS. When carrying out a PESTLE the notion of a Disaster Management Systems (DMS) in line with political, economic, social, technological, legislative and environmental factors can be applied to the overall development of DMS. Politically on the international arena the basic view of implementing security and safety by using a DMS through political measures is focusing on the viewpoint that there should be safety and stability with the introduction of DMS.

Politically to implement a DMS there is a need to have a consistent political agenda which is in align with the DMS agenda.

Politically to implement a DMS it is important to address the system in terms of the environment and protecting borders by increasing the level of understanding in reason with risk, greater level of understanding of risks and the notion of safer, greater independent and resilient environments are becoming more of a necessity.

DMS implementation it is essential to strengthen the focus of resilience which allows for a holistic and integrated approach which includes the key areas for a DMS to work effectively. The areas for consideration here are focused on the prevention and mitigation, preparedness, response and recovery factors. The concepts of disaster management systems are a clear and focused approach to creating a fundamental result and approach to co-ordinated structure across the government bodies in line with a consistent structure. DMS are required to address and initially allow for the set objectives for governmental approaches and structure which are imperative to understand threats and hazards.

DMS enables an institution or environment to consider links associated with its external environment. Systems are thus implemented in an organisational construct which are fundamentally based on internal organisational factors. The general distinction between internal and external aspects of systems, have to be considered and applied to organisational theories. The focus on internal and external factors associated with DMS when used within the construct of business impact analysis allows for considerations to be applied to the environment in terms of risk in association with DMS planning. Documentation at strategic level does need to be limited in terms of length so as to minimise confusion. An effective DMS would not need to have a complicated set of documentation. It is however, necessary to create a high level plan which looks at addressing emergency planning at operational level. Numerous global organisations have specific and detailed planning documentation. The employment of a DMS needs to complement existing plans which are in place. In particular, the integration and employment of DMS in accordance with disaster management requirements.

WHY PESTLE?

Existing work in this research are interesting with different approaches to DMS (Al-marri and Ramachandran 2009; Chandrasekhar, Zang, Xiao 2014). Chandrasekhar, Zang and Xio (2014) have proposed nontraditional approach of participation by local people and communities to speed up the recovery. However, for creating a systematic approach to disaster planning, we need to use very precise means of analysis the eavery countries cirtical parameters such as strengths, challenges, future planning and risks (natural disasters). Therefore, PESTLE model has been quite popular for large communities such as the whole nation (MarketLine 2015). Organisations find themselves functioning in an environment which is constantly changing and evolving. The need to analyse the concerns and thus amending the method the organisation addresses these concerns is based around a fundamental strategy. It is essential to analyse the organisations external environment. An organisation itself needs to identify external factors within the environment which could impact on the organisation. The PESTLE analysis provides a framework that enables an investigation of the external environment. The PESTLE tool is a powerful technique for analysing the organisational environment. Once the PESTLE is used within an organisational construct it clearly identifies areas that focus on internal changes to the organisation. Political: It is essential to keep abreast of potential policy changes in any government. There may-be a change in government priorities for example environmental regulations. Economic: Considering the economic investment for the types of disaster management systems in place is an essential activity which needs to be considered. Social: Issues which have an impact on the market and population growth are required for DMS as it is imperative to gain understanding of the societal impact on the environment for which the DMS is being developed for. Technological: Technological factors can be divided into key areas. Automation, cost saving, outsourcing, growth of networking capabilities. The evasive side of the growth of technology. Legal: Focus on current and impeding legislation. There is a view of

ensuring organisations understanding the notion of how laws can have an impact on DMS. Environmental: The concerns focused on the environment protection ae considerably important especially in todays ever changing environment. Particularly in areas such as weather, climate, geographical location. For example natural disasters, weather cycles such as monsoons. Physical conditions with the extent and maturity of a country's infrastructure. Weather conditions could cause logistical problems at certain times of the year. As with the other PESTLE factors there is a requirement to look at potential changes to weather patterns. These ecological and environmental aspects can have consequences that are on the social and economic level. MarketLine (2015) provides an extensive application of PESTEL model for structures in Japan. Each PESTEL factors explored on four main parameters such as current strengths, challenges, future prospects, and future risks. Environmental factors include infrastructure, cyclical weather, disposal of materials, energy availability and cost and the ecological consequences of production processes. To summarise, this paper aims to maximise the benefits of PESTLE analysis it should be used on a regular basis within an organisation to enable the identification of trends. The impact of a certain external factor may have more severe consequences for a particular division. The PESTLE technique can help clarify why change is needed and identify potential options.

PESTLE analysis is not a new phenomenon within business environments however, it is something that has not been largely explored within the context of Disaster Management Systems. PESTLE focuses on political, environmental, social, technological, economical and legal aspects of any given organizational environment. It is widely known that many businesses have in the last few years suffered greatly and lost tens of thousands of dollars on account of both man-made and natural disasters. Man-made disasters have included: the bombing of the World Trade Centre and the Oklahoma City Government Building as well as the corruption and damage to various Information Technology systems and their data, information and processing. Natural disasters have included: the earthquakes in Southern California and the San Francisco Bay Area; Hurricane Hugo and Andrew; and floods in the mid-west (Aljazeera, 2005). Disasters like these could clearly take place in the future and it is for this reason that one needs to consider if the incorporation of a Disaster Management System (DMS); and system could be an effective means of protecting businesses from different types of disasters. It is possible to argue that all businesses and Information Technology departments should be involved in Disaster Management System, implementing, testing and updating. Furthermore, the use of DMSs should be encouraged so that in time all Information Technology departments come to accept such systems as a necessity. At times, certain information technology and automated information systems are prone to interruptions that can greatly disrupt the efficient running of such systems. If the Information Technology Contingency Plan was to be adopted by businesses, this problem could be resolved and would put in place useful technical procedures that ensure systems recover quickly from any troublesome disruptions. It is the DMS that determines what planning practices should be implemented by businesses in order to create an efficient Information Technology contingency plan. Although such practices are on the whole sufficient for most business, it is important to acknowledge that some businesses may need to make use of other practices to deal with certain extra needs. This article does not take into account the DMS for supercomputers and wireless networks, but even so the majority of the practices put forth are applicable to these systems.

Earlier work has focused on a more generic mode for emergency-response system and contingency planning for natural disaster and IT security management systems (Al-marri and Ramachandran 2009; Ramachandran & Orange, 2008). In this work, we have developed a global model for Disaster recover planning and management which can be customized and applied to a variety of disasters prone systems such natural, emergency, IT/Network/Security, Data recovery, and incident-response systems. Our approach to data collection and evaluation include a combination of ethnography, grounded

theory, and questionnaire, which we believe, is more effective.

International human actions – the risk associated with chemical, nuclear or other hazards, resulting from deliberate actions – e.g. terrorism, sabotage. Unintentional human actions – the risks associated with chemical, nuclear or other hazards, resulting from accidents – e.g. hazardous materials, spill or chemical release, explosion, fire, water control, structure, building and dam. Environmentally – analysing consequences / impacts – that affect many set objectives. Does the risk have the potential to impact on large scale geographical areas? Does the risk have the potential to impact the health of the population - does the risk have the potential to identify impact on the borders, and the impact on the environment in the long run? Develop strategic emergency management planning – building blocks, strategic emergency management plan – the step focuses on an informed emergency management approach for the institution. Inputs should include emergency management planning considerations and assumptions. All hazard risk assessment establish an emergency management structure. Each institution should establish an emergency management governance structure. Confirming strategic priorities it is important to ensure that the governance structure is aligned to the overall governance structure. Identify assumptions, constraints and limitations. The planning team should aim to clearly identify the planning constraints and institutional limitations that will influence the subsequent development. Identify prevention / mitigation, preparedness response and recovery requirements and opportunities.

II. A Model for Disaster Management System and Risk Management Process using PESTLE

Risk management has been widely used in various projects. However, risk management for NDS is more complex and harder to predict. Therefore, this section aims to structure DMS as part of risk management process for NDS. A variety of procedures are adopted to appropriately identify, control and reduce risks to Information Technology systems. Fallara (2003) has proposed a similar approach to disaster recover planning as part of the risk management as they are crucial to any disaster recovery. However, we have proposed a more structured approach to Disaster Management System as an element of risk management. In order to effectively manage risks to Information Technology contingency planning, it is necessary that the following risk management actions are taken: Firstly, it is important to investigate whether the concerned system has any weaknesses that could lead to it being damaged or destroyed and subsequently to take the required precautions. There are three types of threats in particular that could harm weak or insecure systems:

- Natural: this includes fires, floods, tornados and hurricanes.
- Human: this involves terrorist attacks, human mistakes, and risk from hackers.
- Environmental: this includes software gaining errors, equipment ceasing to work and power failures.

Secondly, it is essential to asses any residual risks in order to form an effective contingency plan. Figure 1 shows Disaster Recovery System: which shows the process of putting into place the necessary security precautions, forming a contingency plan and putting the DRS into action when any incident occurs.

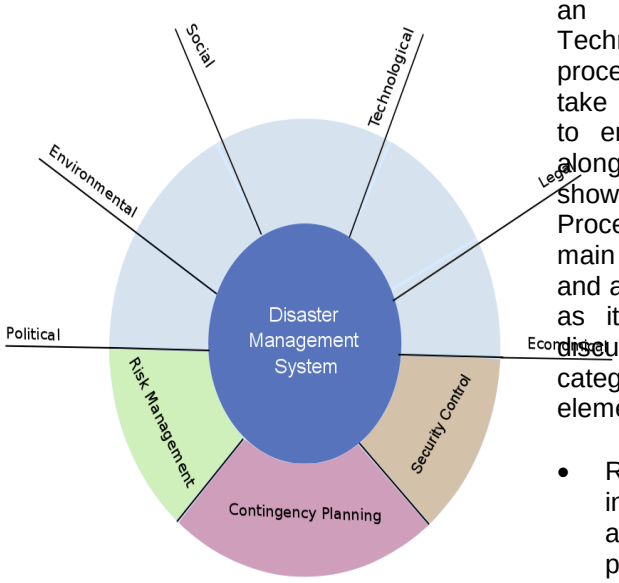

Figure 1 Disaster Management System Using PESTLE

It is important that analyses of risks to Information Technology systems are taken to ensure that the risks to Information Technology systems are properly identified. In this way, it is possible for risks to be allocated with a risk level that predicts how high at risk systems are to various threats and how serious such threats may be to systems. The measures put in place to deal with risks clearly have to be constantly examined and updated by the people in charge of Information Technology contingency planning since Information Technology systems may constantly be forced to face new dangers from various threats. Information Technology contingency planning involves a larger range of measures than DMS to help Information Technology systems survive disasters (Van & Turoff, 2007). In particular, Information Technology contingency planning need to be focused on guaranteeing that organisations and businesses are able to survive disasters as well as plans for ways of dealing with any disasters that may hit Information Technology systems, business processes and facilities. Although there has been no general consent on what would constitute effective Information Technology contingency planning, the fact that there is an inbuilt link between Information Technology systems and business processes shows that every plan should take into account the two at the same time to ensure that the two work effectively alongside one another. Generally, Figure 2 shows the Disaster Risk Management Process (cycle). The DRMP consists of four main processes/stages such as identifying and analyzing risks, etc. explain the diagram as it appears on the picture and then discuss sub-processes/steps within those categories. It is composed of following main elements:

- Risk location and examination: this involves assessing the cause, nature and behaviour of the threat and, in particular, determining how serious it is.
- Knowledge management: this involves raising awareness about potential risks, putting in place education and training programs, extensive research on ways of preventing disasters.
- Political commitment to a disaster reduction policy: this includes ensuring that laws are drawn up to ensure that such policies are adhered to.
- Taking active measures to reduce risks: this could include planning and building protective structures like dams and dikes.
- Cautionary methods for disasters: this could include ensuring that people are supplied with the knowledge and information required (ESPON, 2005) to take the necessary precautions against disasters.
- Preparation for disasters: this includes making sure that people are able to cope with any disasters that may occur. For example, this could involve creating a suitable plan to evacuate people from buildings.
- Repairs and rebuilding: this includes seeing to it that areas that have been hit by disasters are repaired and that the people affected by disasters are given the required assistance so that they may deal with whatever situation they may be in.

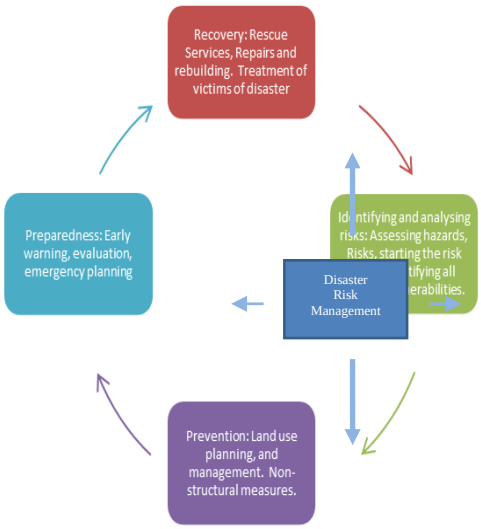

Figure 2 Disaster Risk Management Process

The above main elements can lead one to conclude that disaster recovery management involves firstly actions taken prior to a disaster. It is essential to assess what risks businesses or places may be prone to and to put in place the required measures to ensure that businesses and places are defended effectively against such risks. Secondly, disaster risk management involves actions taken at the time of a disaster including assisting those areas and people involved in disasters. Thirdly, it must involve taking action after disasters occur and it must ensure that the necessary repairs and reconstructions are put in place to improve the areas hit by disasters. It is essential to take into account the technical capabilities, costs and the social and environmental consequences when assessing ways of reducing risks ((Committee, 2005), 2005) and not just the actions taken prior to disasters, which is at times the only concern of disaster risk management (Deutsche, 2004).

The Business Continuity Plan (BCP) and Disaster Management System (DMS) Strategies. The Business Continuity Plan may be designed generally for all the main business processes or specifically for a single business process. It also takes into account the value of Information Technology systems to business processes. Although the DMS does not take into account small disruptions that Information Technology contingency plans often treat, it does very often include a plan designed for Information Technology systems and can be used as a way of restoring target systems, applications or facilities in more suitable locations. If required by a business or organisation, several DMSs may be included with the BCP. Risk management template is one the structured means of identifying risk elements, impact factors, and relevant actions required (Table 1). Our impact factor consists of a number risk levels:

Critical which is a highest form of risk and therefore immediate action is required.

- High
- Medium
- Low

Critical Aspects	Impact Factor	Recover/Contingency Plan	Team Responsible
Evacuate people from the place of incident such as a building	Critical	Call emergency evacuation team of professional experts such as Army personals.	Establishment Manager

Table 1 Risk Assessment Template for Recovery

III. Effective Disaster Recovery System Plan (DSP)

It is clear that teamwork is essential for the creation of effective disaster recovery programs. This section proposes disaster recover plan, which is essential to structure DSR activities. It is essential that teams working on such programs must adhere to health and safety guidelines and must be briefed on exactly what the requirements are for the businesses or systems that need protection from disasters[13]. It is crucial that teams also take constantly monitor what protection is needed by examining whether there are any new potential threats; this means that teams must constantly be assessing whether the resources they have to deal with disasters are sufficient for creating effective disaster recovery systems. It is important that there are three separate teams to deal with the three separate phases of Disaster Management System (Fallara, 2003). It is essential that there is one team that examines what requirements are needed to prepare systems and

businesses for disasters; another team that actually puts in place and manages a Disaster Management System; and a third implementation team that carries out the action. Figure 3 shows DMS Team Management and the detailed phases are:

- Phase 1 Requirements what is meant and what is to be done
- Phase 2 team to create and manage a Disaster Management System
- Phase 3 Implementation team to take action

DMS MANAGEMENT TEAM		
Phase 1: Requirements DMS Requirement Team	Phase 2: Planning DMS Planning Team	Phase 3: Implementation DMS Implementation Team

Table 2 Effective Disaster Management System Planning Cycle

It is essential that an assessment is made of what sort of skills need to be possessed by the team members of each phase and also what resources are required by every team. A coherent structure also needs to be put in place so that every team know exactly what its objectives and responsibilities are; this is essential for the smooth and effective running of the Disaster Management System (Fledrich & Burghardt, 2007). Various developments to the traditional hot site disaster recovery business took place in the 1980s, which was partly due to the fact that compute hardware was becoming cheaper and that technology was centered largely around personal computers (Rehak, 1994). Although these plans in the 1980s were able to deal with the use of mainframe computers, it was not until later that plans were put in place to take into account communications networks. Indeed the plans designed today differ greatly from the 1980s as it is now a requirement that managers prepare themselves for any potential risks and computer systems need to be able to operate at all times. This means that if any disaster should occur, it is essential that the systems affected are restored in a number of hours instead of days and that any lost date is fully restored. Such changes are mainly due to various government regulations, union contracts and the demands from customers. Today, technology plays a massive role on most businesses with various companies having both local and remote basis connections to their main computer.

Additionally government institutions are responsible for conducting mandate specific risk assessments, including risks to critical infrastructure. The key to any emergency planning is awareness of the potential situations that could impose risks on the organisation and to assess those risks on the organisation and to assess those risks on the terms of their impact and potential mitigation measures. Assess the internal environment. Understanding the internal context is essential to confirm that the risk assessment approach meets the needs of the institution and of its internal stakeholders. It is the environment in which the institution operates to achieve its objectives and which can be influenced by the institution to manage risk. The internal context may include the capabilities, understood in terms of resources and knowledge, capital, time, people, processes, systems, technologies, including capability improvement process, information systems, information flows and decision making processes, internal risks and vulnerabilities. It is important to identify, appraise and prioritise all institutional assets. Assets can be both tangible and intangible and can be assessed in terms of importance, value and sensitivity. With respect to know threats and hazards a vulnerability exists when there is a situation or circumstance that if left unchanged may result in loss of life or may affect the confidentiality, integrity or availability of other mission critical systems. Examples of conditions that maybe considered vulnerabilities include – personal issues, high turnover, insufficient secondary or support processes and existing disaster management systems that are immature and have not been tested. Considering all hazard risk assessment. Each institution has its own risk assessment process of informing decision making. Each organisation has its own strategic and operational objectives with each being exposed to its own unique risks and each having its own information and resource limitations. Therefore the risk assessment process is tailored to each institution. Risk translates into events or circumstances that if they materialise, could negatively affect achievement and objectives. The hazard

risk domain is divided into three risk areas – natural hazards intentional human actions and unintentional human actions. Natural hazards – the risk associated with natural geographical, meteorological or biological – e.g. landslides, flood, drought, pandemic influenza, foot and mouth disease, insect infestation (ZIKA Virus).

IV. Evaluation and Validation of the Model

This section will explain the evaluation model. According to Fledrich, et al 2007 focuses on gathering data about the usability of a design or product by specific group of users for a particular activity with a specified environment or work context. The Environmental problems can be considered as a contributed element of causing instability. It hinders economic development; displaces populations; contributes in the increase of weapons of mass destruction; and enhances the growth of undesirable elements. Some countries are considered as environmental troubled regions. They suffer from water shortages, hazardous materials, oil spills in the Gulf, shipping incidents, and transmission of new diseases. Disaster recovery Management Activity Model and the contingency and continuity-planning model for recovery actions have been discussed. The requirements of workforce safety will be also explored. In addition to that, advices, suggestion on how the emergency managers could be developed, and the way to create excellent communication and co-operation with involved organizations and individuals will be presented. This PESTLE DMS model provides an explanation of the use of emerging technology, the role of people and their culture, and global support. It is vital to understand and analyze the operation of power within the context of evaluation in order to identify the approaches, tools and methods which can contribute in improving the practice of information system evaluation. According to Ramachandran et al (2008), Less that, 25% of the managers believe that the organisation did very well in handling the disaster contingency and around 14% only said the organisation very poor in handling the disaster contingency (Ramachandran, 2009a).

This paper encourages emergency managers to apply business continuity plan and Disaster Management System along with other newer technologies in the work. It offers ideas and possible actions, which can be adopted by the emergency managers when dealing with disasters. For that reason, the paper will present issues such as business continuity plan (BCP), Disaster Management System (DMS), workforce, education, and information technology facilities and insurance (Al-Marri & Ramachandran, 2009). It gives example of how to apply business continuity plan and Disaster Management Systems at lowest cost.

An environmental scan is necessary to gather and analyse information and typically consider both internal and external factors. The planning context for additional information on the factors to consider. Scanning can be done on a regular scheduled basis, such as annually or a continuous basis for environmental factors. The planning context for additional information on the factors to consider. Scanning can be done on a regular scheduled basis, such as annually or on a continuous basis for environmental factor that are dynamic or that are of greatest interest to the institutions. As part of the environmental scan, the institution defines the internal and external parameters to be taken into account when managing the risk and setting the scope and risk criteria for the remaining risk assessment process. It sets the time, scope and scale and contributes the adoption of an approach that is appropriate to the situation of the institutions and to the risks affecting the achievement of its objectives.

V. Conclusions

Today Disaster Management Systems have developed significantly since their early days when it was the company data centre that provided the most protection. They are now able to ensure that all the main operating components are protected by the innovative usage of a corporate-wide risk management approach. Many lives and vast amounts of money can be saved if disaster

plan is designed efficiently for a company's so long as all the phases of the planning procedure are stuck to and developed. Indeed emergency and security management programs may only be truly effective if the plan is properly designed. Teamwork and cooperation between all members of an organisation is essential for preventing disasters and it is clear that good contingency business planning effectively depends on everyone preparing for disasters and responding immediately to them.

On the whole DMS's are implemented to be aligned to existing plans, procedures and internal procedures and internal processes which are required to address the emergency support functions in line with other policy documentation. Additional to this DMS's are implemented to focus on hazards, which look at risk management measures which are applied to preventing and mitigation, preparedness, response and recovery. There is a further requirement to ensure that greater understanding can be achieved from these systems and typically in line with an emergency, which additionally refers to an immediate event, including events under the umbrella of an IT incident, which requires immediate co-ordination of actions which are related to individuals in relation to property, which is required to protect the health, safety or welfare of individuals or in line with limiting damage to property or the environment. There are some risked based functions which are aimed at addressing the DMS which is required to support the prevention and mitigation of ensuring there is readiness for response to and recovery from emergencies. The areas addressed here are in line with functions undertaking DMS's in areas such as environmental scans and updates of environmental factors; additionally there should be on-going regular all hazard risk assessments which additionally underpin the whole government approach to the whole government approach and the collection and analysis of government response. There are additional steps to consider before the implementation of a DMS can occur. These are in relation to identifying training and skills requirements analysis.

It is necessary to carry out an environmental scan, which is required to look at assessing both the internal and external environment factors. There is a need to look at stakeholder positions and concerns they may have in line with positions and issues that arise. There is a need to identify the existing plans and address the openings in gaps in meeting institutional requirements and looks at the positions and issues of stakeholders. Additionally there is a need to address the assets and services list to complete and update critical assets and services. The criticality assessment and business impact analysis is essential when updating the business impact analysis. Completion of threats and hazards need to be identified in terms of vulnerabilities that are required to identify current safeguards. Conducting hazards and risk assessments are needed to outline the hazards applied to conducting all hazards. To identify risks, establishing a risk register, analysing risks, evaluating probability, likelihood of occurrence and analyse the probability to evaluate the likelihood of occurrence, where it is necessary to analyse the consequences and impacts (Daniel, Guttorm, Teqje, & Arne, 2003). Evaluating risks and prioritising risks to identify risk prevention with mitigation options. Evaluating risks, prioritise risks and identify risk prevention / mitigation in line with preparedness and in the main focusing on opportunities with the notion of addressing requirements which encompass threats, hazards and specific plans. It is essential for far more engagement with the internal and external stakeholders, in order that information can be updated and refined within the DMS. The process of planning and recognising responsibilities in terms of DMS processes is necessary for the DMS to be used effectively. Establishing a governance structure, confirming priorities for strategic assumptions, constraints and limitations. The DMS needs to be focused on central activities which provides clear integration and inter departmental DMS. The DMS can trigger the planning stages of the system with clear links to integration and co-ordinating of other internal DMS plans. The planning stages can be prompted the DMS cycle for planning and it can be initiated by ensuring the DMS is responsive to human actions. The DMS can vary between government institutions, and in terms of the composition of the DMS. The

planning stages should consist of the necessary skills and experience to develop and apply key skills and experiences necessary to develop the DMS.

The areas to consider would entail the following:

- Identify team members and fundamental areas
- Establish authority and skills set requirements
- Establish authority and terms of reference

Ownership needs to be considered in terms of the obligations and requirements of the existing legislation and policies which are in place. The DMS planning team needs to have a clear level of authority and direction. The DMS process should be carried out as part of an institutions strategic and business planning process which will be applied to allow for the alignment. Following this the next focus is on implementation at specific documentation.

VI. References

Aljazeera. (2005). Retrieved from http://english.aljazeera.net/NR/exeres/A46E0B05-1DC7-4852-83A1-

Al-Marri, S., & Ramachandran, M. (2009). Global Emergency Response System Using GIS. In *Enterprise Information Systems and Implementing IT.*

Chandrasekhar, D., Zang, Y., and Xiao, Y. (2014) Nontraditional Participation in Disaster Recovery Planning: Cases From China, India, and the US, Journal of the American Planning Association, Autumn 2014, Vol. 80, No. 4

Daniel, L. M., Guttorm, S., Teqje, B., & Arne, S. (2003). Evaluating the Quality of Information Business Contingency Planning Models. *Empirical Testing of a Conceptual Model Quality Framework*. Retrieved from Evaluating the Quality of Information Business Contingency Planning Models.

Deutsche, G. F. (2004). Guidelines: Risk Analysis - A Basis for Disaster Risk Management. *Eschborn*.

ESPON, M. (2005). *The Spatial Effects and Management of Natural and Technological Hazards in Europe.* European Spatial Observation Network.

Fallara, P. (2003). Disaster Management System. *IEEE Potential*.

Fledrich, F., & Burghardt, P. (2007). Agent Based Systems for Disaster Management. *Communications of the ACM*.

MarketLine (2015) Japan In-depth PESTLE insights, REFERENCE CODE: ML00002-018, www.marketline.com

Ramachandran, M. (2009). The Role of Information Technology Managers in the Significant Company in case of Natural Deisasters in Qatar. In *Handbook of Software Engineering Researh and Productivity Technologies: Implications of Globalisation.*

Ramachandran, M., & Orange, G. (2008). Information Systems Model fo global emergency-response systemin context of natural Disaster Recovery Management System. *Geo- Information Technology for Natural Disaster Management and Rehabilitation.* Bagkok.

Rehak, R. H. (1994). Disaster Recovery Then and Now: Consideration for Contingency Planning. *Risk Management*.

Van, D. W., & Turoff, M. (2007). Emergency Response Systems: Emerging Trends and Technologies. *Communications of the ACM*